# Steganalysis of the methods of concealing information in graphic containers

**Yaroslav L. Grachev[1]*, Valentina G. Sidorenko[1, 2]**

*[1] Russian University of Transport, Moscow, Russian Federation, [2] HSE University, Moscow, Russian Federation*
**yaroslav446@mail.ru*

*Yaroslav L. Grachev*

*Valentina G. Sidorenko*

**Abstract. Aim.** *Today, there is a pressing matter of protection against steganography-based attacks against information systems. These attacks present a danger as they use the most common data files – especially graphics files – as containers that deliver malicious code to a system or cause a leak of sensitive information. Developing methods of detecting such hidden information is the responsibility of a special subsection of steganography, the steganalysis. Such methods should be extensively used in computer forensics as part of security incident investigation, as well as in automated security systems with integrated modules for analysing data files for malicious or dangerous information. An important feature of such activities is the need to examine a wide variety of elements and containing files. In particular, it is required to verify not only the colour values of the pixels in images, but their frequency characteristics as well. This raises a number of important questions associated with the best practices of applying steganalysis algorithms and making correct conclusions based on the outputs. The paper aims to briefly analyse the most important and relevant methods of steganalysis, both spatial and frequency, as well as to make conclusions regarding their performance and ways to analyse the outputs based on the test results of the software that implements such methods.* **Methods.** *The steganalysis of concealment within the least significant bits of an image's pixels uses Pearson's Chi-square statistical analysis, as well as the Regular-Singular method that involves signature analysis of pixel groups and analytical geometry tools for estimating the relative volume of the hidden message. The Koch-Zhao method of steganalysis is used for the purpose of detecting information embedded in the frequency-domain image representation. It also allows identifying the parameters required for extracting the hidden message.* **Results.** *A software suite was created that includes the software implementations of the analysed methods. The suite was submitted to a number of tests in order to evaluate the outputs of the examined methods. For the purpose of testing, a sample of images of various formats was compiled, in which information was embedded using a number of methods. Based on the results of the sample file analysis, conclusions were made regarding the efficiency of the analysed methods and interpretation of the outputs.* **Conclusion.** *Based on the test results, conclusions were made on the accuracy of the steganalysis methods in cases of varied size of the embedded message and methods of its concealment. The patterns identified with the help of the analysis outputs allowed defining a number of rules for translating the outputs into conclusions on the identification of the fact of detection of hidden information and estimation of its size.*

**Keywords:** *steganalysis, chi-square method, RS method, Koch-Zhao method, stegocontainer.*

**For citation:** *Grachev Ya.L., Sidorenko V.G. Steganalysis of the methods of concealing information in graphic containers. Dependability 2021;3: 39-46. https://doi.org/10.21683/1729-2646-2021-21-3-39-46*

**Received on:** *12.02.2021 /* **Upon revision:** *16.07.2021 /* **For printing:** *17.09.2021.*

## Introduction

Currently, graphics files and data account for a significant share of the network traffic and can be found everywhere, not only as images posted at various network resources, but also as elements of graphical interfaces and design solutions, components of more complex data formats, and many more.

At the same time, the recent years saw a significant growth of malicious software that attacks information systems using steganography, i.e., methods of concealing the fact of transmission of a secret message [1]. Normally, such attacks use image files as containers for delivering potentially hazardous data. That is due to the fact that significant amounts of data can be concealed within them without making any distortions visible to the human eye.

Steganalysis is one of the disciplines of steganography that studies the ways of detecting secretly transmitted information within an analysed information object. Secretly transmitted information is usually understood as information concealed using certain steganographic methods. Additionally, steganalysis also studies the ways and feasibility of extracting concealed information in the process of its detection in the absence of the required input data [2].

Despite the great variety of algorithms of concealing the fact of information transmission in graphics files, almost all of them come down to a number of basic steganographic methods. Those include the method of concealing within the least significant bits of pixels, as well as the Koch-Zhao method that encodes information within an image's representation in the frequency domain [2, 3]. Most other steganographic methods are modifications or variants of those two.

In order to enable the detection of information concealed using the above methods, a number of steganalysis techniques have been developed, whose software implementation allows automating the process of analysis and conducting it without any human involvement (unlike, for example, in the case of various visual attacks).

## 1. Methods of steganalysis

### 1.1. The Chi-square method

A method of attacking a stegosystem using Chi-square analysis was proposed and described by Andreas Westfeld and Andreas Pfitzmann in 1999. This method is designed for detecting information concealed through the method of least significant bits (LSB).

First, the concept of pairs of values (PoV) is introduced. Each pair of values is a pair of bytes that encode the colour intensities that differ by only one least significant bit. Essentially, the LSB method performs transformations within such pairs, changing, if necessary, the byte value from the original to the "adjacent" one in the respective PoV [4].

The idea of this method of analysis is based on the assumption that, within an empty container, the probability of a simultaneous appearance of both values of each pair is low. Therefore, significantly different is the number of colour intensity values that differ by the least significant bit [4]. In other words, for an empty container, the difference in the number of occurrences of the two values of a single pair is significant. Therefore, it is for all POVs. The number of occurrences of each value is also called frequency.

As the theoretically expected distribution, the sequence of the arithmetic mean frequency values of all pairs is chosen. Since, in case of concealmen t in the LSB, the frequencies are only redistributed within a pair and the sum of the pair's frequencies remains unchanged. Therefore, the arithmetic mean frequency value within the PoV remains constant.

The observed sample is understood as a sequence consisting of only the even or only odd values of all PoVs, which is due to the requirement of further comparison of the distribution of such samples with the theoretically predicted distribution as part of Chi-square criterion calculation. In this context, the only relevant factor is the difference between a pair's mean frequency and any frequency observed within such pair.

Thus, the theoretically expected sequence of values made up of pair averages is such for both an empty and a populated container. The degree of similarity between the distribution of the observed sample and the theoretically expected distribution thus becomes the measure of the probability of a steganographic embedding within a container. If a Chi-square estimate allows concluding that the deviations from the theoretically expected distribution are insignificant, that strongly suggests the presence of embedded information.

This method of steganalysis is more efficient if applied not to an entire image, but parts of it. In most cases, the image is divided into blocks of about 1% of the total image area or into conventional lines of the pixel matrix. The latter method allows seeing the approximate beginning and end of the sequentially embedded message.

Although the smallest visible distortions are caused by changes of the blue colour channel pixels, the methods of concealing in the LSB allow using all three channels simultaneously due to the fact that the human eye poorly detects colour changes in case of inversion of the least significant bits of a pixel [5]. In this context, the average probability of concealed information should be calculated for all three colour channels of an analysed image block. Even if concealment was only done in a single channel, the average probability will be noticeably non-vanishing and will allow concluding on the presence of concealed information within such block of pixels.

### 1.2. The RS method

The Regular-Singular method for identifying steganographically concealed messages was proposed by Andreas Pfitzmann, Jessica Fridrich and Miroslav Goljan in 2001. The method is based on the analysis of disjoint groups of $n$ adjacent pixels. $n$ is even [6]. Once the groups have been identified, a regularity function is introduced. That is a function that corresponds a single real number to a single group

and shows the regularity of the group's pixels. The value of the regularity function should be greater the noisier the pixel group is.

As the regularity function, the sum of absolute differences (sum of value differences) of adjacent pixels of a group is chosen:

$$f(G) = f(g_1, g_2, \ldots, g_n) = \sum_{i=1}^{n-1} |g_{i+1} - g_i|, \qquad (1)$$

where $G$ is a pixel group;

$g_i$ is the $i$-th element of the pixel group G;

$n$ is the number of pixels in the group.

After calculating the regularity values for all groups of the analysed image, a group of flipping functions is defined. Those functions correspond to the following set of properties:

1) $\forall x \in P : F(F(x)) = x,\ P = \{0, 255\};;$

2) $F_{\text{dr}} : 0 \leftrightarrow 1, 2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255;$

3) $F_{\text{inv}} : -1 \leftrightarrow 0, 1 \leftrightarrow 2, \ldots, 255 \leftrightarrow 256;$

The group of flipping functions $F$ consists of the direct $F_{\text{dr}}$, the inverse $F_{\text{inv}}$ and the zero $F_0$.

The flipping functions emulate the addition of reversible noise, amplify outliers in a group and reduce its regularity [2].

In order to apply those functions (also called "flipping") to the values of a group's pixels, a mask is used that describes the group of flipping functions applied to the pixel group. A mask is a group of $n$ values, each of which is selected out of three: –1, 0 or 1. Each of them encodes one of the three flipping functions: value "–1" corresponds to $F_{\text{inv}}$, "0" corresponds to $F_0$, "1" corresponds to $F_{\text{dr}}$. Thus, in the process of flipping, a pixel of a group is subject to a flipping function that corresponds to it in the mask.

Upon the application of flipping functions to a group, the current values of the regularity function are compared to those before the flipping. Based on that comparison, the group belongs to one of the classes: regular, singular, unusable:

if $f(F(G)) > f(G)$, then $f \in R$ (the group is regular);

if $f(F(G)) < f(G)$, then $f \in S$ (the group is singular);

if $f(F(G)) = f(G)$, then $f \in U$ (the group is unusable).

For each group, flipping is done twice, i.e., with a direct and an inverted mask. Upon the classification for all groups, a number of quantitative characteristics are calculated:

number of regular groups for mask $M$: $R_M$;

number of singular groups for mask $M$: $S_M$;

number of regular groups for inverse mask $-M$: $R_{-M}$;

number of singular groups for inverse mask $-M$: $S_{-M}$.

All the above characteristics are defined as relative values, i.e., as percentages of the total number of groups $k$. Thus, $R_M + S_M \le 1$ and $R_{-M} + S_{-M} \le 1$. The fundamental hypothesis of this method is the assumption that in an empty container, the numbers of single-class groups for the regular and inverse mask are: $R_M \cong R_{-M}$ and $S_M \cong S_{-M}$.

Fig. 1 shows a typical representation of what is called an RS diagram, a graph of values $R_M$, $S_M$, $R_{-M}$ and $S_{-M}$ depending on the number of pixels with inverted LSBs in the image [6]. $P$ in Fig. 1 and further refers to the percentage of population of a stegocontainer with a concealed message (relative length of message). Plotted on the x axis is the percentage of pixels with inverted LSBs, plotted on the y axis is the percentage of groups of regular and singular classes of the direct and inverted masks (out of the total number of groups).

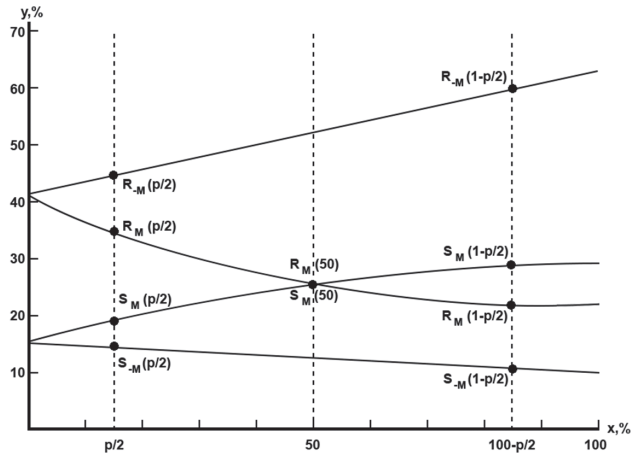


Fig. 1. RS diagram

Based on the information on this typical behaviour of the graphs of quantitative characteristic of the groups, further calculations are performed that allow estimating the relative length of the concealed message.

If the relative length of the concealed message is $p$, then, since $p$ is a random bit stream, on average, $p/2$ LSBs are inverted in an image. In such case, a 100% population of a stegocontainer causes a situation when $p/2$=50%. The inversion of a half of the LSBs means that the difference between the number of regular and singular groups will come down to zero. Then $R_M \cong S_M$, which can be seen in the RS diagram.

The numerical measurements of the groups correspond to the points of the RS graph $R_M(p/2)$, $S_M(p/2)$, $R_{-M}(p/2)$ and $S_{-M}(p/2)$. The calculated numerical characteristics of the groups for the same image after all of its LSBs have been inverted will correspond to points $R_M(1-p/2)$, $S_M(1-p/2)$, $R_{-M}(1-p/2)$ and $S_{-M}(1-p/2)$.

Then, the RS method suggests approximating the curves that pass through points $R_{-M}(p/2)$, $R_M(1-p/2)$ and $S_{-M}(p/2)$, $S_{-M}(1-p/2)$ respectively, with straight lines. The curves that pass through points $S_M(p/2)$, $S_M(1-p/2)$ and $R_M(p/2)$, $R_M(1-p/2)$ are approximated with square parabolas subject to the existing points of intersection of lines and parabolas. A parabola and a line that correspond to the same mask have an intersection point on the x axis of the RS diagram, while the parabolas, as it was mentioned above, intersect if $p/2$=50%.

In order to estimate the relative length of the message $p$, a system of 11 equations with 11 unknown variables must be solved. Such variables are two coefficients for each of the two lines, three coefficients for each of the two parabolas and the value $p$. The system includes 8 straight-line or parabola equations for the 8 previously found points, 2 equations for the intersection points of parabolas and corresponding strait lines and an equation for the intersection

point of parabolas. The system's solution allows finding the value $p$ [6].

The key feature of the RS method is that it analyses the quantitative characteristics of small groups of pixels. Due to that, it, while not being able to detect the area of potential embedding, can detect a concealment made in random bits, rather than sequentially.

## 1.3. Steganalysis using the Koch-Zhao method

This type of analysis is intended for detecting messages embedded into container images using the Koch-Zhao method. The method searches for information encoded in the frequency-domain representations of images.

The frequency-domain representations of an image are generated by calculating the discrete cosine transform (DCT) coefficients, for which the image is divided into blocks of 8×8 pixels, upon which a bivariate DCT is performed on each block producing a matrix of 64 coefficients [7].

In the resulting matrix, the coefficient in the upper left corner that corresponds to the zero frequency (matrix element indexed (0; 0)) is called the *DC* coefficient. It defines the primary shade (average colour intensity) of the entire block. All other resulting coefficients are called *AC* coefficients and express the frequency of colour intensity variation along different directions in the selected block (horizontal and vertical) [8].

Thus, each matrix of DCT coefficients is divided into three subsets, i.e., low-frequency, mid-frequency and high-frequency (from the upper left to the lower right corner of the matrix).

The low-frequency coefficients have a greater effect on the colour intensity of pixels. Accordingly, any variations and transformations to the DCT coefficients are done in the mid- or high-frequency regions.

One of the most important tasks that needs to be addressed when attempting the detection of a Koch-Zhao embedding is to make a correct conclusion regarding which DCT coefficients were used for such embedding. Since the application of the Koch-Zhao method involves concealing information in one of the sets of mid-frequency components, the basic analysis operations are performed for each of these sets individually [9].

Since the bits of the concealed message are encoded through the difference between the absolute values of the selected coefficients, the absolute values of such differences for all the image blocks must be calculated first:

$$C_i = \left\| D_i(k1,k2) \right| - \left| D_i(k2,k1) \right\|, \quad (2)$$

where $D_i(x,y)$ is the value of the DCT coefficient indexed $(x, y)$ in the $i$-th block.

What is calculated at this stage is not the difference between the absolute coefficient values, but rather their absolute values. That is due to the fact that bit encoding is defined by crossing the threshold value $P$ for zero and $-P$ for one [9].

Despite the possibility of fluctuations in the form of different peak values $C_i$ in blocks that were not used to encode bits of a concealed message, the actual blocks used for embedding are recognized by the relatively long continuous section of peak values.

Fig. 2 shows the histograms of values $C_i$ for the same empty and populated container, respectively. Along the x axis are the indexes of blocks, along the y axis are the values $C_i$ of the corresponding blocks.

As we can see, the histograms of the dependence of value $C_i$ on the block number for an empty and populated containers will differ in that the latter has a step-like section.

For the purpose of obtaining the limits of the area containing the embedding, a sequence of modules of the histogram value differences is made, where the two largest values should correspond to the limits of the area of embedding.

However, if the image is large, detecting a small concealed message (especially one encoded with a low threshold value) may be significantly complicated due to the "random" peak values of sequence $C_i$. That may be due to the use of graphics formats that allow compression, the differences in the accuracy of DCT calculation on the encoding and

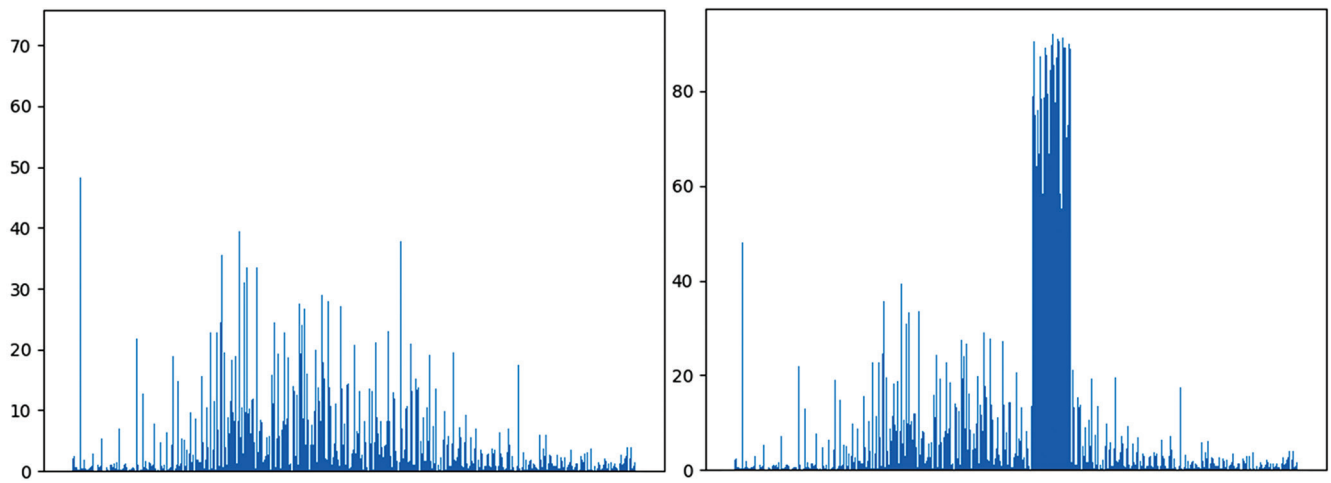


Fig. 2. Histograms of values $C_i$ of an empty and populated container

analysing devices, as well as possible distortions and losses in the process of image transmission.

In order to reduce the probability of failure of the algorithm of embedding detection due to such "noise", the histograms are to be pre-analysed taking into account the fact that the embedded message corresponds to the continuous section of the peak values, i.e., to find the longest such section.

Thus, it can be concluded regarding the presence of an embedded message and the limits of the concealed message can be defined from the block index values. In order to calculate the encoding threshold, the minimal value out of $C_i$ must be found within the detected area of embedding. This value can be used to retrieve information.

The above analysis procedures are to be performed for each of the assumed pairs of DCT coefficients. Normally, those are the following sets of coefficient pairs: (3;4) and (4;3), (3;5) and (5;3), as well as (4;5) and (5;4) [8]. Out of the obtained results, the one should be selected that corresponds to the highest detected value of the encoding threshold $P$.

## 2. Results of method performance testing

The above methods of steganalysis were tested using the software suite developed by the authors that implements all three detection algorithms.

As part of the testing program, a sample of 1600 image files was analysed, in which, using one of the three methods (serial variation of the LSB method, pseudo-random variation of the LSB method, the Koch-Zhao method), one of nine earlier prepared text files was concealed or no information was concealed at all.

For each sample file, an analysis was performed using all three implemented methods: Chi-square, RS and steganalysis of Koch-Zhao concealment. The methods' performance in the form of relative (for the first two) or the absolute (for the last) estimated length of the message concealed in the image were compared with the actual sizes of the message concealed in each container.

Average deviation means the arithmetic average of the absolute values of the difference between the detected relative size of the concealed image and the actual relative size. The mean deviations for the Chi-square and RS methods are shown in Table 1.

**Table 1. Average deviations for the Chi-square and RS methods**

| Name of method | For empty containers, % | Sequential LSB, % | Pseudorandom LSB, % |
|---|---|---|---|
| Chi-square | 0.105 | 1.411 | 22.225 |
| RS | 4.055 | 22.996 | 4.403 |

As it can be seen, the Chi-square method has almost no false positives on empty containers, while RS, in average, shows an extremely low level of occupancy, about 4%.

It can also be seen that the Chi-square method demonstrates good accuracy when detecting sequential embedding in the least significant bits (on average, the error of estimation of the message size is only about 1.4%), while in case of pseudorandom embedding the error is slightly less than a quarter of the size of the container, i.e., only allows detecting or suspecting the fact of embedding.

Regular-Singular, on the contrary, demonstrates good accuracy in identifying pseudorandom concealment and extremely poorly estimates the size of sequentially embedded messages.

In order to better evaluate the efficiency of hidden message size estimation using Chi-square and RS, the mean deviations for various rates of relative container occupancy were calculated. Those values are shown in Tables 2 and 3.

**Table 2. Mean deviations for various occupancy rates for the Chi-square method**

| Occupancy rate | Mean deviation in case of sequential LSB, % | Mean deviation in case of pseudorandom LSB, % |
|---|---|---|
| 100% | 0.609 | 0.000 |
| 90% – 100% | 2.107 | 26.665 |
| 80% – 90% | 3.678 | 61.536 |
| 70% – 80% | 2.851 | 69.184 |
| 60% – 70% | 5.013 | 54.700 |
| 50% – 60% | 3.248 | 52.638 |
| 40% – 50% | 1.783 | 44.272 |
| 30% – 40% | 1.761 | 35.669 |
| 20% – 30% | 1.635 | 24.164 |
| 10% – 20% | 1.019 | 13.543 |
| 0% – 10% | 0.366 | 5.384 |

Based on the above findings, a number of patterns can be identified. The accuracy of identification of the size of a message that is concealed using the sequential method is quite high for Chi-square in case of any message size. The largest deviation of about 5% is observed in cases when containers are 60-70% full.

At the same time, Chi-square enables an extremely accurate identification of the size of a concealed pseudo-random message if it is 100% of the size of the container. If it is below 100%, but above 90%, the method definitely identifies an embedding, but the error of message size estimation is significant. If the occupancy is below 90%, Chi-square is not always able to detect a concealment. Its average deviation in some cases is roughly equivalent to the relative message size. If the occupancy is below 60%, Chi-square shows the worst results in case of pseudo-random concealment. If the occupancy is between 60% and 90%, it is able to identify embedding, but estimates the message size with enormous errors.

**Table 3. Mean deviations for various occupancy rates for the Chi-square method**

| Occupancy rate | Mean deviation in case of sequential LSB, % | Mean deviation in case of pseudorandom LSB, % |
|---|---|---|
| 100% | 70.501 | 11.593 |
| 90% – 100% | 67.184 | 8.060 |
| 80% – 90% | 57.385 | 4.112 |
| 70% – 80% | 50.704 | 1.806 |
| 60% – 70% | 40.795 | 1.638 |
| 50% – 60% | 29.291 | 1.264 |
| 40% – 50% | 21.286 | 2.977 |
| 30% – 40% | 11.476 | 2.985 |
| 20% – 30% | 6.277 | 2.166 |
| 10% – 20% | 5.254 | 3.832 |
| 0% – 10% | 3.894 | 3.722 |

RS shows good accuracy of pseudo-random embedding identification. However, if the occupancy is below 10%, it is not always able to identify a concealment (the average deviation is about 3.7%, while the deviation for empty containers is about 4.4%). If the occupancy is between 20% and 80%, the method demonstrates high accuracy (less than 3% of average deviation). If the size of a pseudo-randomly concealed message is above 80%, the error of the RS method is noticeably higher. It is the greater the larger is the size of the embedded information. The method demonstrates a higher error when the occupancy is 10-20%.

While evaluating the size of a sequentially concealed message, RS shows far worse results and has an average deviation the higher the higher the occupancy rate. At the same time, a message size below 10% in most cases prevents a clear identification of a fact of concealment (same as with pseudo-randomly concealed information and taking into account the average deviation for empty containers).

If the occupancy is above 10%, RS will estimate the size of the hidden message on average at about 15-30% of the container size, which allows making a clear conclusion of the fact of embedding, yet its size is identified very inaccurately.

In order to evaluate the performance of the algorithm of steganalysis of Koch-Zhao concealments, the number of correctly recognized images was identified, for which the algorithm correctly estimated the size of the hidden message, the incorrectly recognized, for which the algorithm retrieved an incorrect, yet non-zero message size value, and the unrecognised, for which the algorithm retrieved 0 in a situation when the image contained actual concealed information.

The above characteristics are presented in Table 4.

Using the Koch-Zhao method, all the empty containers were correctly identified as images that do not contain concealed information.

As it can be seen from the table, in more than 90% of cases the algorithm correctly identified the size of the embedded message, and therefore, it could be likely extracted. In most other cases, the size was identified incorrectly, which prevents the extraction of concealed data (at least without manual operations), yet it allows making a clear conclusion regarding the presence of concealment in the frequency domain. 1.3% of the images remained completely unidentified, which may be evidence of a low chosen information embedding threshold or high level of noise that causes outlying DCT matrix value differences that complicate the identification of the embedding area.

The analysis of the test results also showed that the Koch-Zhao steganalysis did not reveal a single case of concealment in the spatial domain of an image (in the least significant bits), while the Chi-Square and RS failed to produce a result that would allow identifying the fact of embedding in the image representation in the frequency domain.

## 3. Conclusions regarding the use of the methods of steganalysis

The above findings show that in order to obtain clear conclusions regarding the presence of embedded information into least significant pixels of an image, both Chi-Square and RS must be used. A comparison of the outputs of both methods in most cases allows identifying the type of embedding, i.e., sequential or pseudo-random,

**Table 4. Characteristics of various result types of the Koch-Zhao concealment analysis**

| Result type | Number | Relative number |
|---|---|---|
| Correctly identified | 277. | 92.3% |
| Incorrectly identified | 19. | 6.3% |
| Not identified | 4. | 1.3% |

as well as more or less accurately estimating the size of the message.

If the Chi-square estimate is below 0.1% and the RS estimate is below 4%, there is no embedding and the container is empty.

If the Chi-square estimate is close to 100%, the container is fully or almost populated. If the RS estimate is about 30% or less, the information is embedded sequentially, if it is about 80% or more, it is embedded pseudo-randomly.

An RS estimate of more than 30% and Chi-square estimate not higher than 30% indicate a pseudo-random embedding. If the RS estimate is less than 80%, it can be considered an almost accurate estimate of the size of the concealed message. Otherwise, it can be reliably assumed that the size of the concealed information exceeds 80%.

If the RS estimate is below 30%, it should be compared with the Chi-square estimate. The latter being times lower or close to zero indicates a pseudo-random embedding with the message size corresponding to the RS estimate. However, if the Chi-square estimate is approximately equal to or greater than the RS estimate, a sequential concealment of information is identified. Accordingly, the size of the concealed data should be considered equal to the Chi-square estimate.

The above rules of output comparison and analysis used in the shown sequence allow covering most combinations of the Chi-square and RS outputs. Outputs that do not fit the rules indicate fluctuations that may be caused by a variety of factors (high image noise, extremely small image size, etc.) and require manual intervention to produce the final output.

The obtained conclusions are graphically represented in Fig. 3. *p* is the final estimate of the size of the concealed message. Shown in blue are the areas of pseudo-random embedding (O.2, O.4, O.5, O.7). Shown in green are the areas of sequential embedding (O.3, O.6). Shown in gray are the areas of criteria values that require further study. The white area (O.1) indicates an empty container.

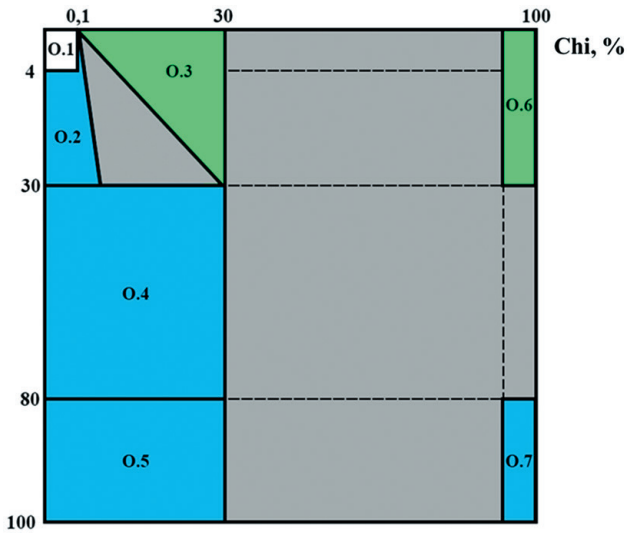


Fig. 3. Graphical representation of outputs

The implemented method of frequency domain steganalysis in most cases allows detecting concealments made using the Koch-Zhao method, however, the size of the concealed message can in a number of situations be identified incorrectly. Therefore, in some cases, extracting information concealed in the frequency domain may require a manual intervention in the form of expert analysis of the histograms of DCT coefficient difference.

Thus, these rules and conclusions can be used in integrated security systems or individual image analysis modules, automatically detecting potentially hazardous graphics files that can carry embedded malicious code or sensitive data.

## Conclusion

The conducted study of the methods of steganalysis enabled their software implementation as a single suite. The suite's testing on a sample of 1600 image files allowed assessing the overall efficiency of the methods, the average errors in the estimation of the length of embedded messages. The tests revealed a number of patterns, a dependence between the outputs of the methods and the size of the hidden messages. The revealed patterns lead to a number of conclusions regarding the performance of the examined methods of steganalysis. They allow correctly evaluating the obtained estimates of the size of hidden information and making conclusions accordingly.

These patterns and conclusions simplify the work of computer forensics experts who use these steganalysis techniques to analyse images. They can also serve as research criteria when graphics files are analysed for hidden information in automated information security systems or their steganalysis modules designed to prevent information leaks through steganographic channels or steganography-based attacks.

As part of the software suite development, the analysed methods of steganalysis were adapted to the existing graphics formats that use the *TrueColor* colour storage format. Besides the detection of concealment in the LSB, estimation of the area and approximate threshold of information embedding into the representation of an image in the frequency domain, the suite also enables automatic attempts of extracting such information even from significantly noisy images. The conclusions regarding the specificity of the examined steganalysis methods in the form of rules for comparing joint analysis outputs allow fine-tuning the criteria of security systems or traffic analysers for the purpose of preventing information security incidents.

## References

1. Varnovsky N.P., Golubev E.A., Logachev O.A. [Modern trends in steganography]. Proceedings of the Conference Mathematics and security of information technologies in MSU, October 28-29, 2004. Moscow: MCCME; 2005.

2. Agranovsky A.V., Balakin A.V., Gribunin V.G. et al. [Steganography, digital watermarks and steganalysis: a monograph]. Moscow: Vuzovskaya kniga; 2009. (in Russ.)

3. Konakhovich G.F., Puzyrenko A.Y. [Computer steganography. Theory and practice]. Kiev: MK-Press; 2006. (in Russ.)

4. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems. Dresden University of Technology, Department of Computer Science. Dresden (Germany): 1999. DOI: 10.1007/10719724_5.

5. Gonzalez R.C., Woods R.E. Digital image processing. Moscow: Tekhnosfera; 2005.

6. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images. New York: Binghamton University; 2001. DOI: 10.1145/1232454.1232466.

7. Khayam S.A. The Discrete Cosine Transform (DCT): Theory and Application. Michigan: Department of Electrical and Computer Engineering, Michigan State University; 2003.

8. Farid H. Digital Image Forensics. *Scientific American*; 2008.

9. Belim S.V., Vilkhovsky D.E. Koch-Zhao algorithm steganalysis. *Mathematical Structures and Modeling* 2018;4(48):113-119. DOI: 10.25513/2222-8772.2018.4.139-119. (in Russ.)

## About the authors

**Yaroslav L. Grachev**, Student, Russian University of Transport, Moscow, Russian Federation, e-mail: yaroslav446@mail.ru

**Valentina G. Sidorenko**, Doctor of Engineering, Professor, Chair Professor, Department of Management and Protection of Information, Russian University of Transport, Chair Professor, Department of Business Informatics, HSE University, Moscow, Russian Federation, e-mail: valenfalk@mail.ru.

## The authors' contribution

**Grachev Ya.L.** Development of a software system that implements the analysed methods of steganalysis, sampling, testing and analysis of the results, conclusions on the performance of the tested methods.

**Sidorenko V.G.** Analysis of methods and principles of steganography, review of the methods of steganalysis.

## Conflict of interests

The authors declare the absence of a conflict of interests.